Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223893475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: VII Número: Edición Especial Artículo no.:58 Período: Noviembre, 2019.

TÍTULO: La informática forense, un camino para potenciar el control interno.

AUTORES:

1. Máster. Franklin W. Montecé Mosquera.
2. Máster. Laura M. Ochoa Escobar.
3. Máster. Freddy M. Jordán Cordones.
4. Máster. Verónica J. Valencia Vargas.

RESUMEN: El acelerado desarrollo tecnológico de la sociedad trae aparejado que las organizaciones se tornen vulnerables a hechos delictivos relacionados con la información digital. Constituye un reto el análisis de los riesgos, evitar la ocurrencia de delitos informáticos y la realización de auditorías como herramientas claves en las actividades de prevención o en la obtención de pruebas. En este contexto, el propósito del trabajo es exponer un procedimiento para la gestión de la informática forense que contribuya a la ejecución de las políticas de control interno de cada organización.

PALABRAS CLAVES: informática forense, riesgos informáticos, toma de decisiones.

TITLE: Computer forensics, a way to enhance internal control.

AUTHORS:

1. Máster. Franklin W. Montecé Mosquera.

2. Máster. Laura M. Ochoa Escobar.

3. Máster. Freddy M. Jordán Cordones.

4. Máster. Verónica J. Valencia Vargas.

ABSTRACT: The accelerated technological development of society entails that organizations become vulnerable to criminal acts related to digital information. It is a challenge to analyze risks, avoid the occurrence of computer crimes, and perform audits as key tools in prevention activities or in obtaining evidence. In this context, the purpose of this work is to develop a procedure for the management of forensic computing that contributes to the execution of the internal control policies of each organization.

KEY WORDS: computer forensics, computer risks, decision making.

INTRODUCCIÓN.

El acelerado desarrollo tecnológico de la sociedad, evidenciado desde mediados del siglo pasado, transforma profundamente las estructuras sociales, laborales, culturales y económicas, en el que desempeña un papel trascendental las Tecnologías de la Información y las Comunicaciones (TIC). El surgimiento de las TIC ha marcado para la humanidad un salto radical en la forma de concebir, desde el diseño de producciones a pequeña y gran escala, hasta las relaciones sociales. Su evolución y desarrollo a pasos agigantados ha permitido que la sociedad haga uso de ellas de forma prácticamente masiva.

Con el surgimiento de la informática como ciencia y luego su desarrollo vertiginoso ha dado lugar a que el uso de las TIC se generalizase en grandes empresas, escuelas, universidades e instituciones gubernamentales, entre otras, por lo que prontamente formó parte de la vida cotidiana a nivel mundial.

Por consiguiente, todo este desarrollo trajo aparejada una dependencia casi total de la informática en la sociedad; así pues, es decisiva en el control de información tanto personal como institucional, para lo cual directivos y personal empresarial deben estar preparados, no solo para su uso por las ventajas que trae para el trabajo profesional, sino para poder controlar eficazmente todos los procesos empresariales.

El surgimiento de las redes de comunicación, ya sean locales, regionales o globales, tiene como máximo exponente la World Wide Web (www) o internet, lo que originó el desarrollo veloz de disímiles formas de comunicación, y por tanto del comercio a nivel mundial, con un incremento de las transacciones e intercambios económicos; en consecuencia, un crecimiento exponencial del acceso a la información. Estos grandes beneficios trajeron aparejados el surgimiento de los delitos y crímenes informáticos, como expresión de una "evolución" en las formas de delinquir, lo que dio lugar tanto a la diversificación de los delitos tradicionales, como a la aparición de nuevos actos ilícitos (Pérez, 2016 y Rodríguez, 2016).

A raíz del rápido crecimiento que han tenido estos crímenes a nivel global surgió la necesidad de crear sistemas capaces de analizar, identificar y documentar las evidencias que podían prevenir y detectar el delito, y garantizar el cumplimiento de las leyes; por lo que surge la informática forense. Esta no es más que la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional, con una finalidad judicial y legal (Cajamarca y Lima, 2018 y Pérez, 2016).

En una organización, el control interno está definido por principios básicos a cumplir, los que responden a intereses propios de una institución, empresa o país. Los mismos se refieren a la delimitación de responsabilidades y procedimientos, cuya incorrecta utilización puede afectar de forma directa e indirecta a los intereses organizacionales.

Las evidencias resultantes de una buena aplicación de la informática forense tributan directamente a una mejor aplicación del control interno en una institución, lo que brinda elementos claves en la determinación, manejo y prevención de irregularidades en las políticas definidas en dicho plan, y coadyuva de esta forma a una eficaz toma de decisiones.

El análisis de los riesgos constituye un reto, así como evitar la ocurrencia de delitos informáticos y la realización de auditorías como herramientas claves en las actividades de prevención o en la obtención de pruebas, luego de ser detectada la existencia de actividades ilícitas y la intrusión de extraños en dichas redes. Para los directivos de las empresas resulta importante tener garantizada las herramientas que les permitan tomar decisiones justas cuando se presentan estos hechos.

Los aspectos señalados anteriormente demuestran la necesidad de tener profesionales competentes para la ejecución de los análisis forenses, además de las herramientas metodológicas adecuadas, diseñadas a partir de las características presentes en el entorno corporativo que será su esfera de actuación profesional. Estos elementos permitirán que los administradores de redes y directivos de las empresas descansen su seguridad informática sobre bases más sólidas.

De acuerdo con lo expuesto y con la finalidad de aportar a las investigaciones que versan sobre el tema, el propósito de este trabajo consiste en desarrollar un procedimiento para la gestión de la informática forense que contribuya a la ejecución de las políticas de control interno de cada organización. Se encuentra distribuido en tres secciones; la primera, “la informática forense”, comenta los fundamentos en los que se basa esta ciencia; la segunda, “situación actual de la informática forense”, enfatiza en su importancia para apoyar los procesos de dirección de las organizaciones y profundiza en el estado de avance de esta rama; por último, la tercera presenta una propuesta de “procedimiento para la gestión de la informática forense”, compuesta por cuatro etapas y pasos que orientan de manera lógica y organizada; el proceder.

DESARROLLO.

La informática forense.

El conocimiento colectivo del término forense ha estado asociado a la medicina siempre, lo que ha propiciado que la informática forense esté relacionada con programas o aplicaciones informáticas que se utilizan en la medicina forense; sin embargo, en la realidad está aplicada a muchas otras ramas de la ciencia como son la Economía y la Informática.

Con el auge de las computadoras y las TIC, la seguridad informática está cada vez más vulnerada, lo que por cierto ha dado lugar a la implementación de una serie de acciones que refuerzan la seguridad; no obstante, no han sido suficientes, ya que los criminales informáticos encuentran nuevas formas para continuar con sus vandálicas acciones.

"El campo de la informática forense se inició en la década de 1980, poco después de que las computadoras personales se convirtieran en una opción viable para los consumidores. En 1984, fue creado un programa del FBI. Conocido por un tiempo como el Programa de Medios Magnéticos, que ahora se conoce como CART (CART, del inglés computer analysis and response team), o análisis de informática y equipo de respuesta" (Cordoba, K., 2014).

Este tipo de informática no nace con el surgimiento de internet o las redes informáticas; sino que surge a partir de la investigación de virus informáticos, con la técnica denominada ingeniería inversa, que puede considerarse el inicio de la informática forense (Rodríguez, 2016; Naharro, Montañés y Barrios, 2018).

La informática forense tiene sus fundamentos en las leyes de la física, la electricidad y el magnetismo. Gracias a fenómenos electromagnéticos, la información se puede almacenar, leer y recuperar, aunque haya sido eliminada. Por otra parte, en la investigación de un crimen se aplican métodos científicos, con procedimientos estrictos, para la recolección, análisis y validación de todo tipo de pruebas

digitales. Es por esto que es posible resaltar el carácter científico de esta rama de la informática (Cajo, Pucuna, Cajo, Coronado y Orozco, 2018; Gómez y Espinoza, 2015).

Existen diversas definiciones para establecer qué es la informática forense, las cuales tienen tantos elementos en común como diferencias, según el criterio de cada autor y el momento en que han sido desarrolladas. Maldonado (2008) plantean que la auditoría forense constituye un conjunto de técnicas que en forma simultánea se aplican para poder obtener las evidencias competentes y relevantes que permitan sustentar las pruebas y testimonios.

Otra de las definiciones plantea que el objetivo del análisis informático forense es realizar un estudio total de todo tipo de evidencia digital que se encuentre involucrada en un incidente (realizar recopilación, preservación, análisis y reporte de la evidencia), con el fin de hacer que cobre valor legal, y que, del mismo modo, sea admisible a la hora de entablar procesos judiciales en los cuales tenga un carácter determinante (Alonso y Esparza, 2017; Bautista, Parra y Guerrero, 2017; Torres, Pedrera y Jiménez, 2017 y Trejo, Álvarez, y Chimbo, 2015).

La informática forense es una ciencia que se utiliza para la detección, recuperación y preservación de evidencia digital. Sin embargo, esto no abarca la totalidad de potencialidades que representa realmente. Tales consideraciones pueden enriquecerse a partir de su carácter científico, y los métodos y herramientas definidos para su aplicación (Torres, 2016 y Villamizar, Orjuela, Adarme, 2015).

Situación actual de la informática forense.

El valor de la información en la sociedad actual aumenta aceleradamente, lo que resulta un pilar esencial para el desarrollo de empresas y organizaciones. Desde este hecho, la informática forense, sus usos y objetivos, adquieren mayor trascendencia, lo que determina impactos negativos o positivos importantes en la sociedad.

Por tanto, la informática forense puede brindar diversa información, como quién estuvo a cargo de los equipos, su historial de manejo, si estos tenían conexión satelital, información financiera, histórica, informativa, mediática, proyectos, planes a futuro y estructura organizativa, entre otros. De ella depende el éxito o fracaso de la investigación. Por el contrario, si la extracción de la información no es obtenida mediante los procedimientos reconocidos de la informática forense, todo lo que se presente carecerá de valor y su veracidad podrá cuestionarse.

Poco a poco, los crímenes informáticos, su prevención y procesamiento son cada vez más importantes en el mundo digital, donde es imprescindible poder conducirse de forma segura en este universo de las TIC para el desarrollo, lo que hace de esta ciencia una herramienta fundamental para la toma de decisiones a nivel corporativo.

Este tema ha adquirido gran importancia dentro del área de la información electrónica, debido al aumento de su valor y al uso que se hace de la misma. La computadora y los sistemas informáticos son fundamentales dentro de esta sociedad moderna y por esta razón favorecen el crecimiento de las organizaciones.

Contrario a lo que se cree, estas mismas herramientas de desarrollo se utilizan para cometer delitos que, al igual que un crimen en la dimensión física, deja evidencias que quedan almacenadas de forma digital; en la mayoría de los casos, dicha información no se puede leer o recolectar por medios comunes o mecanismos tradicionales.

Actualmente, la Organización Internacional de Evidencia Computacional (IOCE, por sus siglas en inglés) es la principal organización que se ha encargado de establecer las pautas a seguir para desarrollar un proceso forense legal en el campo de la informática. Por la generalidad y flexibilidad de sus guías, es la más consultada, y sus establecimientos, los más utilizados.

Además de esta organización, existen otras más, así como empresas que también se han dedicado al estudio de la informática forense, las que de igual forma han emitido documentos orientadores para

los procesos forenses. La mayoría de las intrusiones no se detectan, o se detectan cuando ya es demasiado tarde, o simplemente no se quieren investigar. Solo en aquellos casos en que vale la pena la inversión, se realiza una investigación forense, pues ella, en sí misma no garantiza cerrar exitosamente un caso de crimen informático, las conclusiones no llevan a la captura del delincuente o sencillamente este ya no se encuentra al alcance de las autoridades.

Los resultados de las investigaciones forenses obtenidos por alguna vía, legal o ilegal, son igualmente utilizados para perfilar las acciones de los criminales informáticos. Resulta innegable entonces la necesidad constante de realizar estudios en la informática forense que aporten conocimientos más amplios, y donde se desarrollen instrumentos más eficientes para estudiar y solucionar este nuevo tipo de delito.

Para que estos tipos de investigaciones tengan validez es necesario que se cumpla con ciertas normas y leyes, ya sea a nivel legal o corporativo, puesto que en cada caso existen particularidades que marcan diferencias en cuanto a la aplicación de los procedimientos forenses. En este sentido, la ciencia forense provee de ciertas metodologías básicas que contemplan el correcto manejo de la investigación y de la información.

Las organizaciones encargadas de esta tarea a nivel mundial han elaborado guías para la aplicación de la informática forense que recogen sus mejores prácticas. Tienen como objetivo identificar evidencias digitales con el fin de que puedan ser usadas en una investigación. Dichas guías se basan en métodos científicos para concluir o deducir algo acerca de la información. Presentan una serie de etapas para recuperar la mayor cantidad de fuentes digitales con el fin de asistir en la reconstrucción posterior de eventos. Existen diferentes tipos de planteamientos y estos varían en dependencia del criterio de la institución y personas que definen la guía.

Procedimiento para la gestión de la informática forense.

El procedimiento propuesto sigue un enfoque sistémico; inicia por el reconocimiento de la situación a resolver y transita por cuatro etapas, como se muestra en la figura 1.

Figura1. Procedimiento para gestión de una investigación informática forense.

Fuente: elaboración propia.

En la **etapa 1** se determina un caso de estudio y se analizan los elementos que permitan definir en qué situación se encuentra el o los equipos de cómputo que serán objeto de la investigación, así como los "supuestos hechos", para esclarecer de forma general lo ocurrido; criterios que forman parte de la base de la investigación. Se determina si la investigación es viable, a partir del resultado de entrevistas con el personal involucrado en el proceso, el análisis del tiempo con que se cuenta y los recursos disponibles. Para ello se define el problema y se analiza la disponibilidad de recursos, el hardware necesario para realizar la investigación, según las características de los equipos, y tiempo de ejecución de la investigación.

En la **etapa 2** se lleva a cabo la identificación de recursos, alcance y objetivos necesarios, para garantizar de forma precisa el conocimiento del tipo de evidencia que se busca, dónde encontrarla y cómo proceder para la obtención de la misma sin alterarla o dañarla, para garantizar su autenticidad. Es oportuno tener en cuenta los elementos siguientes:

- Aseguramiento del equipamiento a analizar. Define las medidas de seguridad necesarias para resguardar todo el material que se analizará durante el proceso de investigación. La totalidad de los elementos relacionados con el caso amplía el espacio de búsqueda y aumenta las posibilidades de obtención de evidencias.
- Identificación de debilidades y fortalezas en la configuración y explotación del o los equipos a analizar. Esta información puede obtenerse directamente de los planes de seguridad informática definidos por la institución, así como del libro de incidencias en las verificaciones del cumplimiento del mismo.
- Realización de la investigación preliminar. Entrevistar en detalle el personal que tuvo acceso al equipo o directamente a la información, documentar los posibles momentos y niveles de acceso, controlar los movimientos realizados a los equipos (en caso de haber sido trasladados), así como posibles cambios en las configuraciones de hardware y software.
- Identificación de la tipología de red y equipos informáticos. Se definen los elementos involucrados que puedan estar comprometidos, así como los posibles medios que pudieron utilizarse para realizar el hecho.
- Evaluación del caso. Con la intención de saber si es por violación del plan de seguridad informática definido por la institución o si en efecto es un delito, tiene lugar la verificación de las políticas rectoras para el manejo de información, los equipos que las contienen y los planes de seguridad informática, desde las especificaciones que puedan marcar diferenciaciones entre un departamento y otro, así como los niveles de acceso entre usuarios y dispositivos, ya que no necesariamente un equipo va a ser utilizado por un solo usuario.
- Plan de adquisición de evidencias. Traza las pautas para seguir un orden lógico en el proceso; se determinan que métodos, técnicas y herramientas serán utilizados para la adquisición de datos, se identifica lo más conveniente según las características del proceso, para dar prioridad a la

adquisición de datos volátiles y luego a los no volátiles. Si el equipo se encontraba encendido, es vital no apagarlo hasta que se recolecte la información necesaria, de igual manera si el equipo se encontraba apagado, encenderlo podría representar la pérdida de información, ya que las rutinas del encendido podían haberse alterado para provocar la pérdida de información.

Posteriormente, en la **etapa 3** tiene lugar el análisis y recopilación de información adquirida, desde la interacción usuario-información-hardware. Para ello, es de vital importancia determinar las causas que propiciaron u originaron el incidente; este elemento debe ser documentado durante todo el proceso de realización. Antes de comenzar, es necesario tener todas las copias para realizar las pruebas indispensables a cada una de ellas; en dependencia del tipo de elemento a analizar, así será el procedimiento a seguir. Por consiguiente, se realizarán las siguientes actividades:

- Selección de pruebas a efectuar. Es importante determinar si se procederá al encendido o apagado de los equipos informáticos. Un análisis en encendido (o en vivo) es el que utiliza el sistema operativo y los recursos del mismo para encontrar evidencias; por otra parte, el análisis en apagado (*post mortem*) utiliza herramientas y aplicaciones en un entorno seguro; o sea es el análisis que se cumple con el equipo dedicado exclusivamente para la obtención de pruebas en discos duros o cualquier medio de almacenamiento de información, con fines forenses.
- Utilización de información adicional externa. En caso de ser necesario se debe apoyar en manuales instructivos de servicios y configuraciones para evitar errores futuros. De ahí la importancia de que el especialista sea conocedor del sistema con el cual va a trabajar, así como del hardware que lo contiene, de lo que depende la calidad del resultado final del proceso de investigación.
- Determinación de criterios para la búsqueda de información. Según el tipo de búsqueda definido inicialmente, se fijan los principios que serán aplicados, acordes al tipo de evidencia, ya sea fotografías, documentos, nombres, archivos de video, audio, cadena de caracteres, bases de datos, correos electrónicos, entre otros; se define, además, si esta información está cifrada o no.

Posteriormente, se determina el área de trabajo donde se comenzará el análisis, según el tamaño de la información a analizar. De acuerdo con estos criterios se creará una estructura para los directorios y los archivos recuperados, con especial cuidado al obtener la ruta del fichero recuperado.

- Identificación y recuperación de datos. Debe estar basada en la instalación del sistema operativo, su sistema de archivos y sus aplicaciones; en consecuencia, la recuperación de la información que se realice debe ser lógica y ordenada, y que a su vez permita la selección de una herramienta adecuada para proceder a su análisis y documentar los resultados. Es imperioso extraer la información del sistema de archivos para definir la estructura de sus directorios, atributos, línea de tiempo, nombre, tamaño y localización de los mismos.
- Obtención de datos de las particiones. Este contiene archivos sobrantes del tratamiento de los procesadores de texto, correos electrónicos, cookies, entradas a base de datos y de casi cualquier trabajo que se haya realizado en las últimas sesiones. Lo que genera un problema de seguridad para el usuario, ya que este nunca es consciente de tal almacenamiento transparente. Por otra parte, proporciona datos muy importantes para el especialista encargado de realizar el análisis forense en un equipo de cómputo, que no podrían ser adquiridos de otra manera. El análisis del flujo de datos y procesos se realiza para determinar qué procesos pueden existir, ajenos a los propios del sistema operativo y sus aplicaciones. Arroja elementos importantes para identificar aplicaciones instaladas por personal no autorizado, que en cualquier caso pueden afectar el correcto funcionamiento del sistema o estar presentes para brindar accesos no autorizados al sistema y sus elementos, lo que permite el robo, cambio o falsificación de información.
- Relacionar datos obtenidos y evidencias. Es de interés todo aquello que pueda convertirse en una prueba que constate un hecho de lo ocurrido; se debe realizar una diferenciación entre los datos obtenidos que puedan formar parte de la evidencia y los que simplemente no lo hacen. Una correcta

selección de la misma puede ahorrar tiempo de investigación, además de aportarle seriedad y calidad.

- Detectar y recuperar datos ocultos. Un factor que puede ser de ayuda para efectuar este proceso es el identificar y analizar las aplicaciones instaladas, así como los archivos que generen las mismas, lo que permite llegar con mayor facilidad a determinar los tipos de extensión que deben tener los archivos encontrados, tanto los ocultos como los visibles.
- Evaluación de las configuraciones del perfil de usuario. Proporciona información sobre la configuración del entorno de trabajo de cada usuario, patrones de conducta, historial de internet, cookies, entre otros.
- Identificación de dispositivos de comunicación y defensa perimetral. Determinar los servidores a los que se han accedido desde la máquina objeto de estudio, así como el Firewall, IDS (Intrusion Detection System), IPS (Instrusion Prevention System), detección de anomalías de protocolos, antivirus, valoración de vulnerabilidades, filtrado de contenido, entre otros.

En la **etapa 4** se elabora el documento final, que sustenta las pruebas en un proceso legal. Tiene como objetivo la presentación y entrega de los resultados obtenidos durante la investigación llevada a cabo con el empleo de técnicas de la informática forense. La claridad y calidad con que se presente será la diferencia entre si es aceptada o no como evidencia dentro de un proceso legal. Debe elaborarse estrictamente de acuerdo con las actividades definidas en cada una de las etapas anteriores, lo que evita la omisión de datos.

El procedimiento propuesto fue evaluado a través del criterio de expertos, con el objetivo de comprobar su aporte a la seguridad informática y el control interno en el entorno empresarial. Para ello se empleó el método Delphi con la intención de obtener el consenso de opiniones informadas.

La selección del grupo de expertos estuvo condicionada por su disposición a cooperar. Se envió la encuesta a 20 especialistas para los que se obtuvo el coeficiente de competencia del experto a partir de la autovaloración y de las fuentes de conocimiento.

Los expertos evaluaron como muy adecuada la correspondencia entre objetivo, requerimientos y las diferentes etapas y tareas del procedimiento; así como el orden y la interrelación, claridad y coherencia, lo que le aporta un carácter sistémico. Coincidieron en que constituye una herramienta para garantizar el control interno dentro de cualquier organización y que es pertinente en la orientación sobre la utilización de la informática forense.

CONCLUSIONES.

La informática forense puede aplicarse de manera preventiva o no, mediante la utilización de métodos que permiten detectar de forma oportuna las debilidades de la seguridad informática, garantiza la eficacia del sistema de control interno en cuanto a los procesos que desarrolla y lo vincula a una correcta gestión de riesgos.

El procedimiento que se propone para la gestión de la informática forense contribuye a la ejecución de las políticas de control interno de las organizaciones. Está compuesto de cuatro etapas, en las que se describen las actividades de importancia en cada una de ellas.

Los expertos evaluadores consideraron de muy adecuada la correspondencia entre objetivo, requerimientos, y las diferentes etapas y tareas del procedimiento; así como el orden y la interrelación, claridad y coherencia, lo que le aporta un carácter sistémico. Coincidieron en que constituye una herramienta para garantizar el control interno de cualquier organización y que es pertinente en la orientación sobre la utilización de la informática forense.

REFERENCIAS BIBLIOGRÁFICAS.

1. Alonso, L. A. y Esparza, I. (2017). Los retos procesales de la criminalidad informática desde una perspectiva española. *Novum Jus: Revista Especializada en Sociología Jurídica y Política,* 11 (1), pp.39-72. Recuperado de: https://editorial.ucatolica.edu.co/ojsucatolica/revistas_ucatolica/index.php/Juridica/article/view/1427

2. Bautista, D. R., Parra, J. A. y Guerrero, C. D. (2017). IOT: una aproximación desde ciudad inteligente a universidad inteligente. *Revista Ingenio UFPSO*, 13 (1), pp.9-20.

3. Cajamarca, B. G. L. y Lima, J. S. G. (2018). Desarrollo de una guía metodológica para el análisis forense en equipos de cómputo con Sistema Operativo Mac OS X. *Revista Publicando,* 5 (14), pp.24-67. Recuperado de: https://revistapublicando.org/revista/index.php/crv/article/view/1093

4. Cajo, I. M. H., Pucuna, S. Y., Cajo, B. G. H., Coronado, V. M. O. y Orozco, F. V. S. (2018). Estudio comparativo de las metodologías de análisis forense informático para la examinación de datos en medios digitales. *European Scientific Journal, ESJ,* 14 (18), pp.40-45. Recuperado de: https://www.eujournal.org/index.php/esj/article/view/10956

5. Gómez, E. C. F. y Espinoza, H. A. C. (2014). Cómo responder a un delito informático. *Ciencia Unemi*, 7 (11), pp.43-50. Recuperado de: http://ojs.unemi.edu.ec/index.php/cienciaunemi/article/view/111

6. Maldonado, Y. S. (2008). *Procedimientos de una auditoría forense aplicados a la investigación de lavado de dinero u otros activos en el área de créditos de una institución bancaria*. *(Tesis de pregrado). Universidad de San Carlos de Guatemala Facultad de Ciencias Económicas.* Guatemala. Recuperado de: http://biblioteca.usac.edu.gt/tesis/03/03_3235.pdf

7. Cordoba, K. (2014). Historia de la Informacion Forense. Universidad Nacional Abierta y a Distancia Especializacion en Seguridad Informatica Sibundoy Puntumayo, Colombia. Recuperado de: http://informaticaforensekarolcordoba.blogspot.com/

8. Naharro, F. J., Montañés, C. S. y Barrios, M. S. (2018). La transferencia de los riesgos cibernéticos en empresas internacionales con alto nivel de capitalización bursátil. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 3 (1), pp.67-90. Recuperado de: http://www.uajournals.com/cisdejournal/es/component/content/article.html?layout=edit&id=141

9. Pérez, A. G. (2016). Delitos, internet y redes sociales: perfiles criminales en el ámbito de la Cibercriminalidad social. *Revista Skopein*, 3 (14). Pp.26-7. Recuperado de: https://www.skopein.org/revista-skopein-n-14/

10. Rodríguez, R. A. (2016). El peritaje en tecnologías de información. *Pueblo Continente*, 17 (1), pp33-38.

11. Torres, K. L. I. (2016). La auditoría forense: origen y aproximación como ciencia. *Apuntes Contables*, 18 (1), pp.185-193.

12. Torres, E. A. S., Pedrera, C. J. y Jiménez, M. J. C. (2017). La auditoría forense, una herramienta de control en el sector público y privado del Ecuador. *Sur Academia: Revista Académica-Investigativa del Área Jurídica Social y Administrativa*, 3 (5). Disponible en: https://revistas.unl.edu.ec/index.php/suracademia/article/view/263

13. Trejo, C. A., Álvarez, G. A. D. y Chimbo, K. M. O. (2015). La seguridad jurídica frente a los delitos informáticos. *Avances*, 10 (12), pp.41-41.

14. Villamizar, C., Orjuela, A. y Adarme, M. (2015). Análisis forense en un sistema de información en el marco normativo colombiano. *Investigación e Innovación en Ingenierías*, 3 (1). Recuperado de: http://revistas.unisimon.edu.co/index.php/innovacioning/article/view/2036

DATOS DE LOS AUTORES.

1. **Franklin W. Montecé Mosquera.** Licenciado en Ciencias de la Educación, Magister en Desarrollo Territorial y Docente de UNIANDES, Extensión, Babahoyo. E-mail: ub.franklinmontece@uniandes.edu.ec
2. **Laura M. Ochoa Escobar.** Ingeniera en Sistemas Informáticos, Magister en Informática Empresarial, Coordinadora de la Carrera de Sistemas y Docente de la UNIANDES, Extensión Babahoyo. E-mail: ub.lauraochoa@uniandes.edu.ec
3. **Freddy M. Jordán Cordones.** Ingeniero en Sistemas, Magister en Informática y Docente de UNIANDES, Extensión Babahoyo. E-mail: ub.freddyjordan@uniandes.edu.ec
4. **Verónica J. Valencia Vargas**. Abogada de la República del Ecuador, Magister en Ciencias Penales y Criminológicas y Docente de UNIANDES, Extensión Babahoyo. E-mail: ub.veronicavalencia@uniandes.edu.ec

RECIBIDO: 11 de octubre del 2019. **APROBADO:** 20 de octubre del 2019.